Tutorial 9: Number theory II

Department of Computer Science and Engineering
Hong Kong University of Science and Technology

Idea: "Iterate backwards":

- Starting with step 0, number steps of Euclidean algorithm.
- The equation at step i, will be denoted by $m_i = n_i q_i + r_i$.
- After carrying out step i of Euclidean algorithm, transform it into $r_i = m_i - n_i q_i$.
- Let r_k (step k) be last non-zero remainder.
  Recall that if $r_k = 1, \rightarrow n_0$ has an inverse mod m_0
  (If $r_k \neq 1$, then n_0 has no inverse mod m_0)
- Recall that $m_i = n_{i-1}$ and $n_i = r_{i-1}$.
- Iterate backwards starting with

$$
\begin{aligned}
r_k = 1 = m_k - n_k q_k &= n_{k-1} - r_{k-1} q_k \\
&= n_{k-1} - (m_{k-1} - n_{k-1} q_{k-1}) q_k \\
&= -m_{k-1} q_k + n_{k-1}(1 + q_{k-1} q_k) \ldots
\end{aligned}
$$

Calculating Inverses

Example:

Find the inverse of 15 mod 26.

Step 0:	$26 = 1(15) + 11$	$r_0 = 11 = 26 - 1(15)$
Step 1:	$15 = 1(11) + 4$	$r_1 = 4 \;= 15 - 1(1)$
Step 2:	$11 = 2(4) + 3$	$r_2 = 3 \;= 11 - 2(4)$
Step 3:	$4 = 1(3) + 1$	$r_3 = 1 \;= 4 - 1(3)$

Iterating "backwards" gives:

Step "3":	$1 = 4 - 1(3)$	
Step "2":	$1 = 4 - 1(11 - 2(4))$	$= -1(11) + 3(4)$
Step "1":	$1 = -1(11) + 3(15 - 1(11))$	$= 3(15) - 4(11)$
Step "0":	$1 = 3(15) - 4(26 - 1(15))$	$= -4(26) + 7(15)$

$\boxed{\text{So, } 1 = -4(26) + 7(15) \text{ and } 7 \text{ is the inverse of } 15 \bmod 26.}$

Calculating Inverses

Alternative representation:

k	$=$	j	(q)	$+$	r	x	y
26	$=$	15	(1)	$+$	11	7	-4
15	$=$	11	(1)	$+$	4	-4	3
11	$=$	4	(2)	$+$	3	3	-1
4	$=$	3	(1)	$+$	1	-1	1
3	$=$	1	(3)	$+$	0	1	0

Therefore, we have $26 \cdot -4 + 15 \cdot 7 = 1$ which implies $(15 \cdot 7) \bmod 26 = 1$, and thus 7 is multiplicative inverse of 15 in Z_{26}.

RSA Problem

This problem is on the RSA algorithm for public key cryptography. To generate his keys, Bob starts by picking $p = 37$ and $q = 31$. So, $n = pq = 1147$ and $T = (p-1)(q-1) = 1080$.

(a) Bob's public key is a pair $(e, 1147)$. Which of the following integers can Bob use for e? Why?

(i) 17; (ii) 5; (iii) 49; (iv) 21.

(b) Suppose Bob chooses $e = 47$. Compute his private key d by running the extended GCD algorithm. Show all the steps.

RSA problem

Solution:

(a) (i),(iii). This is because they are the only ones that are relatively prime to T, that is, $gcd(e, T)$ must be 1. (ii) fails because 1080 and 5 are both divisible by 5. (iv) fails because 1080 and 21 are both divisible by 3.

(b) The private key should satisfy $(ed) \bmod T = 1$. i.e. d is multiplicative inverse of e in Z_T. Run the extended GCD algorithm to calculate it:

$$\begin{aligned} 1080 &= 47 \cdot 22 + 46 \\ 47 &= 46 \cdot 1 + 1 \end{aligned}$$

Then,

$$\begin{aligned} 1 &= 47 - 46 \\ &= 47 - (1080 - 47 \cdot 22) \\ &= 23 \cdot 47 + 1080 \cdot (-1) \end{aligned}$$

Thus, $d = 23$.

Inverse Problem

Let p be a prime number (and hence $p \geq 2$).

(a) Show that there are $p^2 - p$ elements with multiplicative inverses in Z_{p^2}.

(b) If x has no multiplicative inverse in Z_{p^2}, what is x^{p^2-p} mod p^2? Explain your answer.

Solution:

(a) The numbers $0, p, 2p, 3p, \ldots, (p-1)p$ have no multiplicative inverses since they are not relatively prime to p^2. But other elements in Z_{p^2} have a multiplicative inverse because they have no factor p and thus they are relatively prime to p^2. So, there are $p^2 - p$ elements with multiplicative inverse in Z_{p^2}.

(b) For any element x with no multiplicative inverse, we can write $x = qp$, where q is an integer and $0 \leq q < p$. So, $x^{p^2-p} = (qp)^{p^2-p} = q^{p^2-p} \cdot p^{p^2-p} = (p^2(q^{p^2-p} \cdot p^{p^2-p-2}))$ which is multiple of p^2, since $p^2 - p \geq 2 \rightarrow p^2 - p - 2 \geq 0$ for any prime p. Thus, $x^{p^2-p} \bmod p^2 = (p^2(q^{p^2-p} \cdot p^{p^2-p-2}))$ mod $p^2 = 0$.